Claims

[c1] Regulated use of encrypted freely distributed files and streams by a user comprising the method steps of:
loading self-installing complex node on user's target computer;
installing said complex node on said user's target computer;
using said encrypted files and streams through secure local decryption by means of said installed node and by means of encrypted credit objects and encrypted policy objects;

[c2] A method of loading said self-installing node of claim 1 on user's target computer from data media such as floppy diskette or CD.

[c3] A method of loading said self-installing node of claim 1 on user's target computer from a network connection.

[c4] A method requiring said self-installing node of claim 1 to obtain a network connection to a node originator to install said node upon said target computer in a unique and complex fashion.

[c5] A method for claim 4 of providing sufficient complexity and variety in said node installation so as to make unauthorized access of any particular data stored by said node practically impossible.

[c6] A method for partially decrypting said encrypted files and streams of claim 1 by the node using the secret key associated with the particular file or stream;

[c7] A method for sending partially decrypted data between said node of claim 1 and the application which uses the decrypted file or stream through channels, which are one or more memory and other exchange locations in the target computer;

[c8] A method for claim 7 of partial decryption within said node using associated secret key and channels, such that said channel communications are initiated with preset channels between said node and said application, and a generated random number is passed over said channels, and used thereafter

to determine channel sequences throughout data transmission from the node to the application;

[c9] A method of updating said node of claim 1 at intervals of time via network connection to provide improvement of security by changing node characteristics such as any of the following: said node secret key, encryption algorithm, channel patterns, unique identification, or calibration of time;

[c10] A method for sending and receiving data through channels described in claim 9 for any data exchange which requires security on the local computer;

[c11] A method of determining policy from said encrypted policy objects and their respective public keys in claim 1;

[c12] A method of receiving and loading said encrypted policy objects and said public keys in claim 11 onto said user's target computer by network connection from a security object source;

[c13] A method of updating said policy object in claim 12 at intervals of time via network connection to keep loaded policy objects current;

[c14] A method of determining credit from said encrypted credit objects and said encrypted secret keys in claim 1;

[c15] A method of receiving and loading said encrypted credit objects and said encrypted secret keys in claim 14 onto said user's target computer by network connection from a security object source;

[c16] A method for decrypting said encrypted secret keys in claim 15 with the target node's secret key;

[c17] A method for securely storing said encrypted credit objects and said decrypted secret keys in claim 17 as distributed throughout the target node's complex memory locations;

[c18] A method for regenerating the node in claim 4 locally through network connection to the node originator. Node modifications are transmitted over

the network and stored on the local computer;

[c19] A method of generating said self-installing complex node in Claim 1 by a node source comprising the steps of:
creating a unique node installation for a computer or digital equipment; the node is of such complexity and uniqueness as to require an installation program;
generating a unique installation program to install said unique node;

[c20] A method of generating said encrypted files and streams in Claim 1 by a file or stream source comprising the steps of:
generating the encrypted files and streams and their identification headers that are associated with encrypted policy objects. Encryption of files and streams may be partial, intermittent or complete;
generating the secret public keys used to decrypt the files and streams;

[c21] A method of generating application which makes use of said node in Claim 1 and said channel jumping in Claim 7 by an application source:

[c22] A method of generating said security objects in Claim 1 by a security object source comprising the steps of:
generating the public keys used to decrypt the policy objects;
generating encrypted policy objects with public keys. The policy objects are associated with a file or stream;
generating encrypted credit objects with or without encrypted secret keys that are associated with either individual or groups of files and or streams;